

REMARKS

The specification has been amended to incorporate a description of new FIG. 5 and FIG. 5 has been added. Proper support for new FIG. 5 can be found in the specification, at least in original claims 41-45. Claim 41 has been amended. Claims 1, 3-11, 13-18, 20-30, 32-35 and 41-47 are pending and under consideration. Claims 1, 13, 18, 30, 41, 46 and 47 are the independent claims. No new matter is presented in this Amendment.

REJECTION UNDER 35 U.S.C §101:

Claims 41-43 are rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter.

Applicants respectfully traverse this rejection for at least the following reasons.

Claim 41 recites a receiver which is part of an apparatus. Accordingly, Applicants respectfully assert that claim 41, as amended, fully complies with requirements of 35 U.S.C. §101 and request that the rejection of independent claim 41 be withdrawn.

Regarding the rejection of claims 42 and 43, it is noted that these claims depend from claim 41 and therefore also comply with the requirements of 35 U.S.C. §101. Accordingly, Applicants respectfully request that the rejection of claims 42 and 43 be withdrawn.

REJECTIONS UNDER 35 U.S.C. §102:

Claims 1, 3-4, 16, 13, 18, 21, 30, and 46 are rejected under 35 U.S.C. §102(e) as being anticipated by Richards (U.S. Patent 6,385,723).

Applicants respectfully traverse this rejection for at least the following reason.

Regarding the rejection of independent claims 1, 18 and 46, it is noted that claims 1, 18 and 46 recite a method of encrypting a text comprising, amongst other novel features, encrypting a first region of a text containing a second encryption key using a first encryption key; encrypting a second region of the text using the second encryption key; transmitting a cipher text comprising the encrypted first and second regions; transmitting the first encryption key, region segmentation information for segmenting the text into the first region and the second region, and

information related to the second encryption key; decrypting the first region of the transmitted cipher text using the transmitted first encryption key and the transmitted region segmentation information; extracting the second encryption key from the decrypted first region using the transmitted information related to the second encryption key; and decrypting the second region of the transmitted cipher text using the extracted second encryption key.

The Office Action relies on Richards for a teaching of encrypting a first region of a text containing a second encryption key using a first encryption key, and cites FIG. 5, items 503, 507 and FIG. 6, item 615 for such teaching. The Office Action further indicates that the first encryption key is public key, mkd_pk, and that the second encryption key is key data 615. The Office Action does not clearly indicate which element of Richards corresponds to the first region of a text which is encrypted, but the Examiner appears to be referring to the KTU cipher text 503, since KTU cipher text portion 503 corresponds to KTU plaintext encrypted with the public key mkd_pk as shown in box 507 (FIG. 5, column 8, lines 40-43).

The Office Action further indicates that Richards teaches decrypting the first region of the transmitted cipher text using the transmitted first encryption key and the transmitted region segmentation information and relies on FIG. 10, item 1003 for such teaching. However, a detailed review of Richards indicates that although the KTU cipher text portion 503 is decrypted, the KTU cipher text is decrypted using a mkd-sk which stands for a MUTLOS key data secret key (column 7, lines 57-65, column 10, lines 66-67, column 11, lines 1-11). In other words, the public key mkd-pk relied by the Examiner, as the first encryption key, does not decrypt the alleged first region, rather the key that decrypts the alleged first region is a secret key, mkd-sk.

Furthermore, it is noted that only the card itself knows the secret key (column 7, lines 57-62) and the secret key is located within the card, even before the alleged first region is transmitted. In other words, the secret key is never transmitted with the encrypted first region of the text, as recited in the independent claims.

Accordingly, Applicants respectfully assert that the rejection of independent claims 1, 18 and 46 under 35 U.S.C. §102(e) should be withdrawn because Richards fails to teach or suggest the novel features recited in the independent claims.

Furthermore, Applicants respectfully assert that the rejection of dependent claims 3, 4 and 16 under 35 U.S.C. §102(e) should be withdrawn at least because of their dependence from claim 1 and the reasons set forth above, and because the dependent claims include additional features which are not taught or suggested by the prior art. Therefore, it is respectfully

submitted that claims 3, 4 and 16 also distinguish over the prior art.

Applicants also respectfully assert that the rejection of dependent claim 21 under 35 U.S.C. §102(e) should be withdrawn at least because of its dependence from claim 18 and the reasons set forth above, and because the dependent claim includes additional features which are not taught or suggested by the prior art. Therefore, it is respectfully submitted that claim 21 also distinguishes over the prior art.

Regarding the rejection of independent claims 13 and 30, it is noted that claims 13 and 30 recite a copy protection method and a method of decrypting an encrypted text comprising, amongst other novel features, decrypting the first region of the cipher text using the transmitted first encryption key and the transmitted region segmentation information; extracting the second encryption key from the decrypted first region using the transmitted second encryption key information; and decrypting the second region of the text using the extracted second encryption key.

As noted above, the Office Action indicates that Richards teaches decrypting the first region of the transmitted cipher text (KTU cipher text 503) using the transmitted first encryption key (public key, mkd_pk) and relies on FIG. 10, item 1003 for such teaching.

However, as noted above, although Richards discloses that the KTU cipher text portion 503 is decrypted, the KTU cipher text is decrypted using a secret key (column 7, lines 57-65, column 10, lines 66-67, column 11, lines 1-11). In other words, the public key mkd-pk relied by the Examiner, as the first encryption key, does not decrypt the first region of text. Richards, rather teaches using a secret key, mkd-sk, to decrypt the text. Furthermore, as also noted above, the secret key used to decrypt the text is known only to the card and is already present in the card even before receiving the encrypted text. In other words, the secret key is never transmitted (column 7, lines 57-62) with the encrypted first region of the text, as recited in the independent claims.

Accordingly, Applicants respectfully assert that the rejection of claims 13 and 30 under 35 U.S.C. § 102(e) should be withdrawn because Richards fails to teach or suggest each feature of independent claims 13 and 30.

REJECTIONS UNDER 35 U.S.C. §103:

Claims 5, 7-11, 17, 15, 20, 22, 24-28, 32, 35, and 47 are rejected under 35 U.S.C. §103(a) as being unpatentable over Richards (U.S. Patent 6,385,723).

Applicants respectfully traverse this rejection for at least the following reasons.

It is noted that claims 5, 7-11 and 17 depend from independent claim 1, and as noted above, Richards fails to teach or suggest the novel features recited in independent claim 1.

Accordingly, Applicants respectfully assert that the rejection of dependent claims 5, 7-11 and 17 under 35 U.S.C. §103(a) should be withdrawn at least because of their dependence from claim 1 and the reasons set forth above, and because the dependent claims include additional features which are not taught or suggested by the prior art. Therefore, it is respectfully submitted that claims 5, 7-11 and 17 also distinguish over the prior art.

Regarding the rejection of claim 15, it is noted that claim 15 depends from independent claim 13, and as noted above, Richards fails to teach or suggest the novel features recited in independent claim 13.

Accordingly, Applicants respectfully assert that the rejection of dependent claim 15 under 35 U.S.C. §103(a) should be withdrawn at least because of its dependence from claim 13 and the reasons set forth above, and because the dependent claim includes additional features which are not taught or suggested by the prior art. Therefore, it is respectfully submitted that claim 15 also distinguishes over the prior art.

Regarding the rejection of claims 20, 22 and 24-28, it is noted that claims 20, 22 and 24-28 depend from independent claim 18, and as noted above, Richards fails to teach or suggest the novel features recited in independent claim 18.

Accordingly, Applicants respectfully assert that the rejection of dependent claims 20, 22 and 24-28 under 35 U.S.C. §103(a) should be withdrawn at least because of their dependence from claim 18 and the reasons set forth above, and because the dependent claims include additional features which are not taught or suggested by the prior art. Therefore, it is respectfully submitted that claims 20, 22 and 24-28 also distinguish over the prior art.

Regarding the rejection of claims 32 and 35, it is noted that claims 32 and 35 depend from independent claim 30, and as noted above, Richards fails to teach or suggest the novel features recited in independent claim 30.

Accordingly, Applicants respectfully assert that the rejection of dependent claims 32 and 35 under 35 U.S.C. §103(a) should be withdrawn at least because of their dependence from claim 30 and the reasons set forth above, and because the dependent claims include additional features which are not taught or suggested by the prior art. Therefore, it is respectfully submitted that claims 32 and 35 also distinguish over the prior art.

Regarding the rejection of independent claim 47, it is noted that claim 47 recites a copy protection method comprising, amongst other novel features, encrypting a first region of a text using a first encryption key; encrypting a second region of the text using a second encryption key; transmitting the encrypted first and second regions, the first encryption key, region segmentation information for segmenting the first and second regions, and information related to the second encryption key; decrypting the first region using the transmitted first encryption key and the transmitted region segmentation information; and decrypting the second region after extracting the second encryption key located in the first encrypted region.

As noted above, the Office Action indicates that Richards teaches decrypting the first region of the transmitted cipher text (KTU cipher text 503) using the transmitted first encryption key (public key, mkd_pk) and relies on FIG. 10, item 1003 for such teaching.

However, as noted above, although Richards discloses that the KTU cipher text portion 503 is decrypted, the KTU cipher text is decrypted using a MUTLOS key data secret key (column 7, lines 57-65, column 10, lines 66-67, column 11, lines 1-11). In other words, the public key mkd-pk relied by the Examiner, as the first encryption key, does not decrypt the first region of text. Richards, rather teaches using a secret key, mkd-sk, to decrypt the text (FIG. 10, item 1003). Furthermore, as noted above, the secret key used to decrypt the text is known only to the card and is already present in the card even before receiving the encrypted text (column 7, lines 57-65). In other words, the secret key is not transmitted with the encrypted first region of the text, as recited in the independent claims.

Accordingly, Applicants respectfully assert that the rejection of claim 47 under 35 U.S.C. § 103(a) should be withdrawn because Richards fails to teach or suggest each feature of independent claim 47.

Claims 6, 14, 23 and 34 are rejected under 35 U.S.C. §103(a) as being unpatentable

over Richards (U.S. Patent 6,385,723) in view of McGough (U.S. Patent 6,445,797).

Regarding the rejection of claims 6, 14, 23 and 34 it is noted that claims 6, 14, 23 and 34 depend from independent claims 1, 13, 18 and 30, respectively, and as noted above, Richards fails to teach or suggest the novel features recited in independent claims 1, 13, 18 and 30.

McGough teaches a method and system for performing secure electronic digital streaming. McGough however fails to teach or suggest the novel features recited in the independent claims and thus fails to cure the deficiencies of Richards.

Accordingly, Applicants respectfully assert that the rejection of dependent claims 6, 14, 23 and 34 under 35 U.S.C. §103(a) should be withdrawn at least because of their dependence from claims 1, 13, 18 and 30 and the reasons set forth above, and because the dependent claims include additional features which are not taught or suggested by the prior art. Therefore, it is respectfully submitted that claims 6, 13, 18 and 30 also distinguish over the prior art.

Claims 29 and 33 are rejected under 35 U.S.C. §103(a) as being unpatentable over Richards (U.S. Patent 6,385,723) in view of applicant's admittance of prior art.

Regarding the rejection of claims 29 and 33 it is noted that claims 29 and 33 depend from independent claims 18 and 30, respectively, and as noted above, Richards fails to teach or suggest the novel features recited in independent claims 18 and 30.

Applicant's Admittance of Prior art also fails to teach or suggest the novel features recited in independent claims 18 and 30 and thus fails to cure the deficiencies of Richards.

Accordingly, Applicants respectfully assert that the rejection of dependent claims 29 and 33 under 35 U.S.C. §103(a) should be withdrawn at least because of their dependence from claims 18 and 30 and the reasons set forth above, and because the dependent claims include additional features which are not taught or suggested by the prior art. Therefore, it is respectfully submitted that claims 29 and 33 also distinguish over the prior art.

Claims 41-45 are rejected under 35 U.S.C. §103(a) as being unpatentable over applicant's admittance of prior art in view of Richards (U.S. Patent 6,385,723).

Regarding the rejection of independent claim 41, it is noted that claim 41 recites an apparatus implementing a copy protection method, the apparatus comprising: an authenticator

to obtain a safe transmission path through which a first encryption key, region segmentation information, and information related to the second encryption key are received; an encryptor to encrypt a text using the first encryption key and the second encryption key, where the second encryption key is extracted from a portion of the text encrypted by the first encryption key; and a decryptor to decrypt a portion of the encrypted text using the first encryption key and the region segmentation information, to extract the second encryption key from the decrypted portion using the information related to the second encryption key, and to decrypt another portion of the encrypted text using the second encryption key.

As noted above, the Office Action indicates that Richards teaches decrypting the first region of the transmitted cipher text (KTU cipher text 503) using the transmitted first encryption key (public key, mkd_pk) and relies on FIG. 10, item 1003 for such teaching.

However, as noted above, although Richards discloses that the KTU cipher text portion 503 is decrypted, the KTU cipher text is decrypted using a MUTLOS key data secret key (column 7, lines 57-65, column 10, lines 66-67, column 11, lines 1-11). In other words, the public key mkd-pk relied by the Examiner, as the first encryption key, does not decrypt the first region of text. Richards, rather teaches using a secret key, mkd-sk, to decrypt the text (FIG. 10, item 1003). Furthermore, as noted above, the secret key used to decrypt the text is known only to the card and is already present in the card even before receiving the encrypted text (column 7, lines 57-65). In other words, the secret key is not transmitted with the encrypted first region of the text, as recited in the independent claims.

Applicant's admittance of prior art also fails to teach or suggest such novel features and therefore fail to cure the deficiencies of Richards.

Accordingly, Applicants respectfully assert that the rejection of claim 41 under 35 U.S.C. § 103(a) should be withdrawn because neither Richards nor applicant's admittance of prior art teach or suggest each feature of independent claim 41.

Furthermore, Applicants respectfully assert that the rejection of dependent claims 42-45 should be withdrawn at least because of their dependence from claim 41 and the reasons set forth above, and because the dependent claims include additional features which are not taught or suggested by the prior art. Therefore, it is respectfully submitted that claims 42-45 also distinguish over the prior art.

CONCLUSION:

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

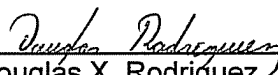
Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 503333.

Respectfully submitted,

STEIN, MCEWEN & BUI, LLP

Date: 3/22/07

By: 
Douglas X. Rodriguez
Registration No. 47,269

1400 Eye St., N.W.
Suite 300
Washington, D.C. 20005
Telephone: (202) 216-9505
Facsimile: (202) 216-9510